Theoretical Computer Science 119 (1993) 127–143
Elsevier

A complete modal proof system for HAL: the Herbrand agent language

Zineb Habbas

Laboratoire d'Informatique fondamentale et d'Intelligence Artificielle, Institut IMAG, Grenoble, France

Abstract

Habbas, Z., A complete modal proof system for HAL: the Herbrand agent language, Theoretical Computer Science 119 (1993) 127–143.

In this paper we present the process algebra HAL (Herbrand agent language) first introduced in (Belmesk et al., 1991). We then propose a modal proof system for HAL without value passing, and prove its correctness and completeness.

Introduction

In the framework of formal specification and verification of concurrent programs, modal and temporal logic has been intensively used during the last few years. Indeed it is a powerful tool to express and to verify a wide spectrum of properties of concurrent programs. However, this formalism has been severely criticized for being global, nonmodular and noncompositional. By that, we mean that in order to formulate and verify a temporal property, we must consider the entire program. Actually, to date there has been no natural way by which temporal specifications that are derived separately for programs p and q could be combined into a temporal specification for their parallel composition, since it is hard to conceive an operator, say $*$ in logic, such that if p satisfies A and q satisfies B then $p \| q$ satisfies $A * B$.

Consequently, even if the temporal logic provides a most useful specification tool, and the "model checking" technique provides a rigorous verification of an existing program, they both offer very little support when dealing with dynamic topology

Correspondence to: Z. Habbas, LIFIA–IMAG, 46 Av. Félix Viallet, 38031 Grenoble Cedex, France. Email: zineb@lifia.imag.fr.

Elsevier Science Publishers B.V.

networks. For this reason, a central activity in successfully applying modal and temporal logic to the development and verification of concurrent programs is somehow to obtain compositionality [11, 12, 18, 19, 22]. To solve this problem we have introduced a new semantic relation named the relativized semantic relation. This strategy has been explored by C. Stirling for building complete modal proof systems for SCCS and CCS.

This paper describes the confrontation of this strategy against the process algebra HAL already defined in [3]. HAL is a process algebra where processes (called Agents) are built by means of process combining operators. This approach is classical. However, HAL differs from CCS, SCCS and all other algebras such as ACP[4] and LOTOS [5] by using unification for communication and by having a special operator for connecting two processes. Furthermore, the concurrency in HAL includes, in addition to arbitrary interleaving, the possibility of simultaneous execution. This semantics is known as the "step semantics" [20].

The paper consists of five sections. The first contains some preliminaries describing and relating Hennessy–Milner logic and bisimulation equivalence. Section 2 presents the subset of the process algebra HAL. In Section 3, we give an operational semantics for HAL without value passing. Section 4 gives two proof systems: Sys_1 and Sys_2. Sys_1 is a proof system for a subset of HAL where the restriction and connection operators are not considered. Sys_2 extends Sys_1 by treating the remaining operators. In Section 5, we give a proof of the completeness of Sys_1 and Sys_2. Comparison with related work and further remarks are given in the last section of the paper.

1. Transition systems, bisimulation and Hennessy–Milner logic

1.1. Transition systems and bisimulation

The work presented in this paper follows up the line of defining processes, concurrent or nondeterministic, by the set of experiments they offer to an observer. We use the model of labelled transition systems, which is a simple model of nondeterminism based on the primitive notion of state and transition. The simple notion of labelled transition systems has proved to be a very good model for operational semantics of programming languages [15].

Definition 1.1 (*Labelled transition system*). A labelled transition system is a structure $T=(P, \text{Act}, \rightarrow)$ where p is a set of states or processes, Act is a set of actions and $\rightarrow \subseteq P \times \text{Act} \times P$ is the transition relation.

For $(p, a, q) \in \rightarrow$, we shall write $p \xrightarrow{a} q$, which may be interpreted as indicating that in state p the system may perform an a action and in so doing evolve to a state q.

A transition system is finitely branching provided that for each $a \in \text{Act}$ the set $\{q : p \xrightarrow{a} q\}$ is finite.

Hennessy and Milner propose that two processes (programs) should be equivalent (have the same meaning) when no amount of finite experimentation distinguishes them. A formal criterion, observational equivalence [13], is proffered which is the same as bisimulation equivalence when T is finitely branching.

Definition 1.2 (*Bisimulation relation*). A binary relation R on P is a bisimulation iff whenever $p\,R\,q$ and $a \in \mathrm{Act}$ then

(1) $\forall a, \forall r\ p \xrightarrow{a} r \Rightarrow \exists s\ q \xrightarrow{a} s$ and $r\,R\,s$,

(2) $\forall a, \forall s\ q \xrightarrow{a} s \Rightarrow \exists r\ p \xrightarrow{a} r\,R\,s$.

A binary relation R is a bisimulation on T if it has the property given in this definition (the identity relation, for instance, is a bisimulation). Such relations give rise to a natural equivalence bisimulation (denoted $\underline{\leftrightarrow}$) on processes in T.

Proposition 1.3. *$\underline{\leftrightarrow}$ is an equivalence relation on P.*

Proof. $\underline{\leftrightarrow}$ is reflexive, symmetric and transitive. The proof of these properties follows easily from the definition of bisimulation. □

Definition 1.4 (*Observational equivalence*). A binary relation $\equiv$ on P is called observational equivalence iff

$p \equiv_0 q$

$p \equiv_{n+1} q$ iff

(1) $p \xrightarrow{a} r \Rightarrow \exists s\ q \xrightarrow{a} s$ and $r \equiv_n s$

(2) $q \xrightarrow{a} s \Rightarrow \exists r\ p \xrightarrow{a} r$ and $r \equiv_n s$

$p \equiv q$ iff $p \equiv_n q\ \forall n \geqslant 0$.

Proposition 1.5. *$\equiv$ is an equivalence relation on P.*

Proof. As bisimulation. □

Theorem 1.6 (Bisimulation and observational equivalence). *If T is a finite branching transition system then $p \equiv q \Leftrightarrow p \underline{\leftrightarrow} q$* [7].

Remark. A more discriminating view of concurrent systems than that offered by interleaving semantics is obtained by modelling concurrency as either arbitrary interleaving or simultaneous execution. *Step semantics* are defined by generalizing the single action transitions $p \xrightarrow{a} q$ from Definition 1.2 of the form $p \xrightarrow{a} q$, where e is a multiset over Act, representing actions occurring concurrently. In particular, we allow actions to occur concurrently with themselves.

This view is taken in calculi like SCCS [14], MEIJE [1], FP2 and HAL. Using this new kind of transition, we obtain step bisimulation equivalence, denoted $\underline{\leftrightarrow}_{\mathrm{step}}$, exactly as the corresponding interleaving bisimulation equivalence.

1.2. Hennessy–Milner logic

Hennessy and Milner have introduced a modal logic (HML) in [7]. We consider a negation-free version of HML.

Definition 2.7 (*Syntax of HML*). The set L_{HML} of HML formulas is given by the following grammar:

$$A, B ::= \mathrm{Tr} \mid \mathrm{Fal} \mid A \vee B \mid A \wedge B \mid \langle a \rangle A \mid [a]A \quad \forall a \in \mathrm{Act}$$

Definition 1.8 (*Semantics of HML*). Let $T=(P, \mathrm{Act}, \rightarrow)$ be a transition system and L_{HML} the language of HML formulas. If $\models$ denotes the satisfaction relation which is defined between processes and formulas, $\models \subseteq P \times L$ is the least relation such that

$p \models \mathrm{Tr}$: $\forall p \in P$

$p \models \mathrm{Fal}$: Never

$p \models A \vee B$ iff $p \models A$ or $p \models B$

$p \models A \wedge B$ iff $p \models A$ and $p \models B$

$p \models \langle a \rangle A$ iff $\exists p$ such that $p \xrightarrow{a} q$ and $q \models A$

$p \models [a]A$ iff $\forall p$: $p \xrightarrow{a} q$ implies $q \models A$

1.3. HML equivalence and bisimulation equivalence

When using temporal logic to reason about parallel or nondeterministic programs, investigations of logic adequacy with the semantics one considers for its (parallel) programs is a general prerequisite. Basically, the logic should not be able to distinguish two programs that we want to consider semantically equivalent, or more formally,

$$p \simeq_s q \Leftrightarrow p \simeq_l q;$$

using $\simeq_s$ to denote a semantics equivalence and $\simeq_l$ to denote a logic equivalence. Let us write

$$\mathrm{Th}(p)=\{A : p \models A\}, \text{ so } p \simeq_l q \Rightarrow \mathrm{Th}(p)=\mathrm{Th}(q).$$

HML is expressively rich. In effect, Hennessy and Milner [7] prove the following characterisation theorem.

Theorem 1.9 (Comparing HML and $\leftrightarrows$). *If T is finite branching then*: $p \simeq_{\mathrm{HML}} q \Leftrightarrow p \leftrightarrows q$.

Definition 1.10 (*The modal height of a formula*). The modal height of a formula is

formally defined as a function $m: L_{\mathrm{HML}} \to \mathbb{N}$:

$$m(\mathrm{Tr}) = m(\mathrm{Fal}) = 0,$$

$$m(A \wedge B) = m(A \vee B) = \max(m(A), m(B)),$$

$$m(\langle a \rangle A) = m([a]A) = 1 + m(A).$$

Remark. We can stratify L_{HML} according to the modal height: $\forall n \in \mathbb{N}$

$$\mathrm{HML}_n = \{A \in \mathrm{HML}: m(A) \leqslant n\},$$

$$\mathrm{HML}_0 \subseteq \mathrm{HML}_1 \subseteq \cdots \subseteq \mathrm{HML}_i \subseteq \cdots.$$

So $\mathrm{HML} = \bigcup_{n \geqslant 0} \mathrm{HML}_n$.

Lemma 1.11. *Let p and q be two processes; then $p \equiv_n q \Leftrightarrow p \simeq_{\mathrm{HML}_n} q$.*

Theorem 1.12. *Let p and q be two processes; then $p \equiv q \Leftrightarrow p \simeq_{\mathrm{HML}} q$.*

The proofs of Lemma 1.11 and Theorem 1.12 are omitted.

2. The process algebra HAL

HAL is a process algebra where processes (called agents) are built by means of process-combining operators. This approach is classical: CSP [8], CCS [13], ACP [4], LOTOS [5], FP2 [9] are examples of process algebras. However, HAL differs from these algebras by using unification to generalize the classical notion of communication by having atomic actions as sets of synchronous communications and by having a slightly different set of operators.

2.1. Atomic actions

An atomic action performed by a HAL agent is a finite, possibly empty, set of synchronous communications.

Ports: K is a family of port names, which are simply denoted by identifiers. If k is a port name, k' ("k prime") is also a port name.

Set of events: Let $k_1, k_2, \ldots, k_n$ be n distinct port names, then $\{k_1, k_2, \ldots, k_n\}$ the set of port names denotes an event. The empty set of port names is denoted by τ. We denote by E the set of events and by $e, e_1, \ldots$ an event or an atomic action.

2.2. Agents

There are nine operators in the algebra of HAL agents. They are within the agent expressions written according to the following grammar, where p and q are agent

expressions, e is a set of offers, K is a connector or a set of pairs of port names ($K=\{\langle ki, li\rangle: 1\leqslant i\leqslant n\}$, x is an identifier and L is a set of port names.

$$p, q ::= \text{Nil} \mid e.p \mid p+q \mid p\|q \mid p[\![K]\!] \mid p\lceil L \mid p' \mid \text{rec}\, x.p \mid x$$

Remark. Parentheses can be used within expressions to make it clear to which operands the operators apply. HAL agents perform sequences of atomic actions.

3. Semantics of HAL

Notation 3.1. Let K be a multiset of pairs of port names, and denote by $\varphi(K)$ the following set of multisets:

$\varphi: K \to \varphi(K)$.
$\emptyset \in \varphi(K)$.
If $\langle a, b\rangle \in K$ then $\{a, b\} \in \varphi(K)$.
If $\{a_i, b_i\} \in \varphi(K)$ and $s \in \varphi(K-\{a_i, b_i\})$ then $\{a_i, b_i\} \pm s \in \varphi(K)$.

We denote by $\pm$ the union of multisets.

3.1. Operational semantics

Operationally we define this semantics in terms of transition systems. This operational semantics defines the behavior of HAL agents. It induces an equivalence relation among agents which is a congruence with respect to the operators of HAL.

The transition system associated with an agent HAL is a tuple $s=(P, E, \to, p_0)$, where P is a set of agents HAL, E is a set of events (set of offers), $\xrightarrow{a}$ is a transition relation, and $p_0 \in P$.

Definition 3.2 (*The definition of* $\to$).

$$\text{E}_\text{M}\ \frac{}{e.p \xrightarrow{e} p} \qquad \text{Sum}_1\ \frac{p \xrightarrow{e} r}{p+q \xrightarrow{e} r} \qquad \text{Sum}_2\ \frac{q \xrightarrow{e} s}{p+q \xrightarrow{e} s}$$

$$\text{Con}_1\ \frac{p \xrightarrow{e} r}{p[\![\langle a, b\rangle]\!] \xrightarrow{e} r[\![\langle a, b\rangle]\!]} \qquad \text{Con}_2\ \frac{p \xrightarrow{e} r}{p[\![\langle a, b\rangle]\!] \xrightarrow{e+\{a,b\}} r[\![\langle a, b\rangle]\!]}$$

$$\text{Par}_1\ \frac{p \xrightarrow{e} r}{p\|q \xrightarrow{e} r\|q} \qquad \text{Par}_2\ \frac{q \xrightarrow{e} s}{p\|q \xrightarrow{e} p\|s} \qquad \text{Par}_3\ \frac{p \xrightarrow{e_1} r \quad q \xrightarrow{e_2} s}{p\|q \xrightarrow{e^1 \pm e^2} r\|s}$$

$$\text{Res}\ \frac{p \xrightarrow{e} r}{p\lceil U \xrightarrow{e} r\lceil U}\ [1] \qquad \text{Rec}\ \frac{p[x:=\text{rec}\, x.p] \xrightarrow{e} r}{\text{rec}\, x.p \xrightarrow{e} r}$$

[1] If $e \cap U = \emptyset$.

4. Compositional modal proof systems

In this section we propose a proof system for the subset of HAL we consider in this paper. To construct this proof system, we proceed in two steps. For this, we subdivide the language of processes into two subsets L_1 and L_2. L_1 is defined on the signature $\Sigma_1 = \{\text{Nil}, ., +, \|, \text{rec}\}$ and L_2 is defined on the signature $\Sigma_2 = \Sigma_1 \cup \{[\![\ ]\!], \lceil\ \}$. After this we propose two proof systems Sys_1 and Sys_2 corresponding to L_1 and L_2, respectively. We establish their results of correctness and completeness.

4.1. *The system* Sys_1

First, we introduce a new semantic relation denoted $\models_B$ (also denoted $B, p \models A$), where $p \models_B A$ signifies: $\forall q\ q \models B \Rightarrow q \| p \models A$. Hence, the construction of sound and complete modal proof systems results in the proof theoretic relations $\vdash$ and $\vdash B$ equivalent to $\models$ and $\models_B$, respectively. The proof rules are reminiscent of the Gentzen introduction rules, except that processes are also introduced. The introduction rules for the connectives of the propositional logic are classical.

The introduction rules given above for action prefixing are at the same time introduction rules for $\langle e \rangle$ and $[e]$:

$$e.p \vdash \langle e \rangle A \quad \text{iff } p \vdash A$$

$$e.p \vdash [e] A \quad \text{iff } p \vdash A$$

Their justification is that $e.p$ must evolve to p under any e experiment.

The restricted introduction rules for the $+$ case depend on the form of A and B and are

$$p+q \vdash \langle e \rangle A \text{ iff } p \vdash \langle e \rangle A \text{ or } q \vdash \langle e \rangle A$$

$$p+q \vdash [e] A \text{ iff } p \vdash [e] A \text{ and } p \vdash [e] A$$

The parallel operator is more difficult to treat since, unlike the $+$ case, restricted versions which depend on the forms of A and B are inadequate. It is for this reason that the relativized semantics has been introduced. Unfortunately, relativizing semantics creates problems for the nondeterministic introduction rule. In effect, as CCS the following rules are not valid for HAL:

$$A, p \models \langle e \rangle B \text{ or } A, q \models \langle e \rangle B \Rightarrow A, p+q \models \langle e \rangle B,$$

$$A, p \models [e] B \text{ and } A, q \models [e] B \Rightarrow A, p+q \models [e] B.$$

The solution we use, suggested by C. Stirling, is to extend HML by two new connectives, $\underline{\langle e \rangle}$ and $\underline{[e]}$. Obviously the semantics of the two connectives semantics

depends upon the semantics of the parallel operator of HAL, and we define it as follows:

Definition 4.1 (*Semantics of the new connectives*).

$p \| q \models \langle \underline{e} \rangle B$ iff $\exists q \xrightarrow{e} q_1$ such that $p \| q_1 \models B$ or $\exists p \xrightarrow{e_1} p_1 \quad q \xrightarrow{e_2} q_1$ such that $e = e_1 \pm e_2$ and $p_1 \| q_1 \models B$.

$p \| q \models [\underline{e}] B$ iff $\forall q \xrightarrow{e} q_1 \quad p \| q_1 \models B$ and $\forall p \xrightarrow{e_1} p_1 \quad \forall q \xrightarrow{e_2} q_1$ such that $e = e \pm e_2$. $p_1 \| q_1 \models B$. $A, p \models \langle \underline{e} \rangle B$ iff $\forall r = A \; r \| p \models \langle \underline{e} \rangle B$.

$A, p \models [\underline{e}] B \; \forall r \models A \; r \| p \models [\underline{e}] B$.

We denote by L the set $L_{\mathrm{HML}} \cup \{\langle \underline{e} \rangle A\} \cup \{[\underline{e}] A\}$. With this extended HML, we successfully treat the $+$ and the $\|$ operators.

Thus rests the case of the Rec combinator. The behavior of $\mathrm{rec}\, x.p$ is fully determined by repeated "unfoldings". An unfolding of $\mathrm{rec}\, x.p$ is $p[\mathrm{rec}\, x.p := x]$. The rules depend upon the modal height of a formula A, denoted $m(A)$ (see Definition 1.10). If $p \models A$ and $m(A) = n$ then A is a property of the evolution of p in response to experimenting whose depth is at most n. When $p = \mathrm{rec}\, x.q$, the guardedness condition on x guarantees that A is at most a property of the nth unfolding of p. We can therefore appeal to standard approximation techniques.

When $p = \mathrm{rec}\, x.q$ then p^n is inductively defined: $(\mathrm{rec}\, x.p)^1 = p$ and $(\mathrm{rec}\, x.p)^{n+1} = p[(\mathrm{rec}\, x.p)^n := x]$.

From these previous techniques the following Rec rules result:

$$p \vdash A \quad \text{iff} \quad p^n \vdash A,$$

$$A, p \vdash B \quad \text{iff} \quad A, p^n \vdash B.$$

In Sys_1, we are concerned with a subset of HAL without restriction and connection.

4.1.1. The proof system Sys_1

$$\mathrm{Ax}_1 \; \frac{}{p \vdash \mathrm{Tr}} \qquad \mathrm{Ax}_2 \; \frac{}{\mathrm{nil} \vdash [e] A} \qquad \mathrm{Ax}_3 \; \frac{}{A, p \vdash \mathrm{Tr}} \qquad \mathrm{Ax}_4 \; \frac{}{\mathrm{Fal}, p \vdash B}$$

$$\mathrm{Ax}_5 \; \frac{}{A, \mathrm{nil} \vdash [\underline{e}] B} \qquad \mathrm{Ax}_6 \; \frac{}{e_1.p \vdash [e] B}\,{}^{2} \qquad \mathrm{Ax}_7 \; \frac{}{[e_1] A, e_2.p \vdash [\underline{e}] B}\,{}^{3}$$

$$\vee \mathrm{I} \quad \frac{p \vdash A}{p \vdash A \vee B} \qquad \frac{p \vdash B}{p \vdash A \vee B} \qquad \frac{A, p \vdash B}{A, p \vdash B \vee C} \qquad \frac{A, p \vdash C}{A, p \vdash B \vee C}$$

$$\frac{A, p \vdash C \quad B, p \vdash C}{A \vee B, p \vdash C}$$

[2] If $e_1 \neq e$.

[3] If $e_1 \pm e_2 \neq e$ and $e_2 \neq e$.

$$\wedge\mathrm{I}\quad \frac{p\vdash A\quad p\vdash B}{p\vdash A\wedge B}\qquad \frac{A,p\vdash C}{A\wedge B,p\vdash C}\qquad \frac{B,p\vdash C}{A\wedge B,p\vdash C}\qquad \frac{A,p\vdash B\quad A,p\vdash C}{A,p\vdash B\wedge C}$$

$$\langle e\rangle\mathrm{I}\quad \frac{p\vdash A}{e.p\vdash\langle e\rangle A}\qquad \frac{A,p\vdash\langle \underline{e}\rangle B}{A,p\vdash\langle e\rangle B}\qquad \frac{A,p\vdash B}{\langle e\rangle A,p\vdash\langle e\rangle B}$$

$$\langle \underline{e}\rangle\mathrm{I}\quad \frac{A,p\vdash B}{A,e.p\vdash\langle \underline{e}\rangle B}\qquad \frac{A,p\vdash B}{\langle e_1\rangle A,e_2.p\vdash\langle \underline{e}\rangle B}\ ^{4}$$

$$[e]\mathrm{I}\quad \frac{p\vdash A}{e.p\vdash[e]A}\qquad \frac{[e]D\wedge E,p\vdash\underline{[e]}B\quad D,p\vdash B}{[e]D\wedge E,p\vdash[e]B}$$

$$\underline{[e]}\mathrm{I}\quad \frac{A,p\vdash B\quad C,p\vdash B}{A\wedge[\tau]C,e.p\vdash\underline{[e]}B}\qquad \frac{A,p\vdash B}{[e_1]A,e_2.p\vdash\underline{[e]}B}\ ^{5}$$

$$+\mathrm{I}(\langle\rangle)\quad \frac{p\vdash\langle e\rangle A}{p+q\vdash\langle e\rangle A}\qquad \frac{q\vdash\langle e\rangle A}{p+q\vdash\langle e\rangle A}\qquad \frac{A,p\vdash\langle \underline{e}\rangle B}{A,p+q\vdash\langle \underline{e}\rangle B}\qquad \frac{A,q\vdash\langle \underline{e}\rangle B}{A,p+q\vdash\langle \underline{e}\rangle B}$$

$$+\mathrm{I}([\,])\quad \frac{p\vdash[e]A\quad q\vdash[e]A}{p+q\vdash[e]A}\qquad \frac{A,p\vdash\underline{[e]}B\quad A,q\vdash\underline{[e]}B}{A,p+q\vdash\underline{[e]}}$$

$$\mathrm{rec}\,\mathrm{I}\quad \frac{(\mathrm{rec}\,x.p)^{m(A)}\vdash A}{\mathrm{rec}\,x.p\vdash A}\qquad \frac{A,(\mathrm{rec}\,x.p)^{m(A)}\vdash B}{A,\mathrm{rec}\,x.p\vdash B}$$

$$\|\mathrm{I}\quad \frac{p\vdash A\quad A,q\vdash B}{p\,\|\,q\vdash B}\qquad \frac{p\vdash A\quad A,q\vdash B}{q\,\|\,p\vdash B}\qquad \frac{A,p\vdash B\quad B,q\vdash C}{A,p\,\|\,q\vdash C}$$

$$\frac{A,p\vdash B\quad B,q\vdash C}{A,q\,\|\,p\vdash C}\ ^{6}\qquad \frac{A,p\vdash B\quad B,q\vdash\underline{[e]}C\quad A,q\vdash D\quad D,p\vdash\underline{[e]}C}{A,p\,\|\,q\vdash\underline{[e]}C}$$

Example 4.2. $\{a,b\}.\mathrm{nil}\,\|\,\{c\}\,\mathrm{nil}\vdash\langle\{a,b,c\}\rangle\mathrm{Tr}$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\mathrm{nil}\vdash\mathrm{Tr}}\,\mathrm{Ax}_1}{\{a,b\}\,\mathrm{nil}\vdash\langle\{a,b\}\rangle\mathrm{Tr}}\,\langle\{a,b\}\rangle\mathrm{I}}{\langle\underline{\{a,b,c\}}\rangle\mathrm{Tr},\{c\}\,\mathrm{nil}\vdash\langle\underline{\{a,b,c\}}\rangle\mathrm{Tr}}\,\langle\underline{\{a,b,c\}}\rangle\mathrm{I}}{\langle\{a,b\}\rangle\mathrm{Tr},\{c\}\,\mathrm{nil}\vdash\langle\{a,b,c\}\rangle\mathrm{Tr}}\,\langle\{a,b,c\}\rangle\mathrm{I}}{\{a,b\}.\,\mathrm{nil}\,\|\,\{c\}\,\mathrm{nil}\vdash\langle\{a,b,c\}\rangle\mathrm{Tr}}\,\|\mathrm{I}$$

[4] $e=e_1\pm e_2$.
[5] $e=e_1\pm e_2$ and $e_1\neq\tau$.
[6] If C is not of the form $\underline{[e]}B$.

4.1.2. Correctness and completeness of Sys_1

Theorem 4.3 (Correctness of Sys_1). *The proof system* Sys_1 *is correct, that is,*
(i) *if* $p \vdash A$ *then* $p \models A$,
(ii) *if* $A, p \vdash B$ *then* $A, p \models B$

Proof. The proof is standard. □

Theorem 4.4 (Completeness of Sys_1). *The proof system* Sys_1 *is complete, that is,*
(i) *if* $p \models A$ *then* $p \vdash A$
(ii) *if* $B \in L_{\mathrm{HML}}$ *and* $A, p \models B$ *then* $\exists C$ *such that* $|C| = |A|$ *and* $C, q \vdash B$.

4.2. The proof system Sys_2

The previous approach cannot naturally be extended to connection since

$$(p \parallel q)[\![K]\!]\lceil U \text{ is not bisimilar to } (p[\![K]\!]\lceil U \parallel q)[\![K]\!]\lceil U.$$

Example 4.5. $p = \{a\}\mathrm{Nil} + \{b\}.\mathrm{Nil}$, $q = \{c\}.\mathrm{Nil}$, $K = \{\langle a, c\rangle\}$, $U = \{a, c\}$. In fact $(p \parallel q)[\![K]\!]\lceil U = \{b\}\mathrm{Nil} + \tau\mathrm{Nil}$ but $(p[\![K]\!]\lceil U \parallel q)[\![K]\!]\lceil U = \{b\}\mathrm{Nil}$.
To solve this problem we introduce the following more generalized semantic relations:

(1) $A, B \models_{K,U} C$ iff $\forall p \models A$, $\forall q \models B$ $(p \parallel q)[\![K]\!]\lceil U \models C$
(2) $A \models_{K,U} C$ iff $\forall p \models A$ $p[\![K]\!]\lceil U \models C$
(3) $p \models_{K,U} C$ iff $p[\![K]\!]\lceil U \models C$

Remark. The introduction of three proof relations which coincide with the previous semantic relations gives us a complete proof system Sys_2.

4.2.1. The proof system Sys_2

$$\mathrm{Ax}_1\ \frac{}{p \vdash_{K,U} \mathrm{Tr}} \qquad \mathrm{Ax}_2\ \frac{}{\mathrm{nil} \vdash_{K,U} [e]A} \qquad \mathrm{Ax}_3\ \frac{}{A, B \vdash_{K,U} \mathrm{Tr}}$$

$$\mathrm{Ax}_4\ \frac{}{e_{1p} \vdash_{K,U} [e]B}\ ^{7} \qquad \mathrm{Ax}_5\ \frac{}{\mathrm{Fal}\, A \vdash_{K,U} B} \qquad \mathrm{Ax}_6\ \frac{}{A, \mathrm{Fal} \vdash_{K,U} B}$$

$$\mathrm{Ax}_7\ \frac{}{[e_1]A, [e_2]B \vdash_{K,U} [e]C}\ ^{8} \qquad \mathrm{Ax}_8\ \frac{}{A \vdash_{K,U} \mathrm{Tr}} \qquad \mathrm{Ax}_9\ \frac{}{\mathrm{Fal} \vdash_{K,U} B}$$

$$\mathrm{Ax}_{10}\ \frac{}{[e_1]A \vdash_{K,U} [e]B}\ ^{9}$$

[7] If $e_1 \neq e \pm s$ for all $s \in \varphi(K)$ or $e \cap U = \emptyset$.
[8] If $(e_2 \neq e \pm s$ and $e_1 \neq e + s$ and $e_1 + e_2 \neq e + s)$ or $e \cap U \neq \emptyset$.
[9] Same as footnote 8.

$\vee$ I $\quad \dfrac{p \vdash_{K,U} A}{p \vdash_{K,U} A \vee B} \qquad \dfrac{p \vdash_{K,U} B}{p \vdash_{K,U} A \vee B} \qquad \dfrac{A \vdash_{K,U} C}{A \vdash_{K,U} C \vee B}$

$$\frac{A \vdash_{K,U} B}{A \vdash_{K,U} B \vee C} \qquad \frac{A \vdash_{K,U} B,\ C \vdash_{K,U} B}{A \vee C \vdash_{K,U} B} \qquad \frac{A, B \vdash_{K,U} C}{A, B \vdash_{K,U} C \vee D}$$

$$\frac{A, B \vdash_{K,U} D}{A, B \vdash_{K,U} C \vee D} \qquad \frac{A, B \vdash_{K,U} C \quad D, B \vdash_{K,U} C}{A \vee D, B \vdash_{K,U} C} \qquad \frac{A, B \vdash_{K,U} C \quad A, D \vdash_{K,U} C}{A, B \vee D \vdash_{K,U} C}$$

$\wedge$ I $\quad \dfrac{p \vdash_{K,U} A \quad p \vdash_{K,U} B}{p \vdash_{K,U} A \wedge B} \qquad \dfrac{A \vdash_{K,U} B \quad A \vdash_{K,U} C}{A \vdash_{K,U} B \wedge C} \qquad \dfrac{A \vdash_{K,U} B}{A \wedge C \vdash_{K,U} B}$

$$\frac{A \vdash_{K,U} B}{C \wedge A \vdash_{K,U} B} \qquad \frac{A, B \vdash_{K,U} C \quad A, B \vdash_{K,U} D}{A, B \vdash_{K,U} C \wedge D} \qquad \frac{A, B \vdash_{K,U} C}{A \wedge D, B \vdash_{K,U} C}$$

$$\frac{A, B \vdash_{K,U} C}{A, B \wedge D \vdash_{K,U} C} \qquad \frac{A, B \vdash_{K,U} C}{D \wedge A, B \vdash_{K,U} C} \qquad \frac{A, B \vdash_{K,U} C}{A, D \wedge B \vdash_{K,U} C}$$

. I $\quad \dfrac{p \vdash_{K,U} A}{e.p \vdash_{K,U} \langle e-s \rangle A}$ [10] $\qquad \dfrac{p \vdash_{K,U} A}{e.p \vdash_{K,U} [e-s] A}$ [11] $\qquad [\![\ ]\!]$ I $\dfrac{p \vdash_{K \cup K',U} A}{p[\![K']\!] \vdash_{K,U} A}$

$\lceil$ I $\dfrac{p \vdash_{K \lceil V, U \cup V} B}{p \lceil V \vdash_{K,U} B}$ [12] $\qquad$ rec I $\dfrac{\mathrm{rec}\, x.p \vdash_{K,U} A}{(\mathrm{rec}\, x.p)^{m(A)} \vdash_{K,U} A}$

$+$ I $\quad \dfrac{p \vdash_{K,U} \langle e \rangle A}{p+q \vdash_{K,U} \langle e \rangle A} \qquad \dfrac{p \vdash_{K,U} [e] A \quad q \vdash_{K,U} [e] A}{p+q \vdash_{K,U} [e] A}$

$\langle e \rangle$ I $\quad \dfrac{A \vdash_{K,U} B}{\langle e \rangle A \vdash_{K,U} \langle e-s \rangle B} \qquad \dfrac{A, B \vdash_{K,U} C}{A, \langle e \rangle B \vdash_{K,U} \langle e-s \rangle C}$ [13]

$$\frac{A, B \vdash_{K,U} C}{\langle e \rangle A, B \vdash_{K,U} \langle e-s \rangle C}\ [14] \qquad \frac{A, B \vdash_{K,U} C}{\langle e_1 \rangle A, \langle e_2 \rangle B \vdash_{K,U} \langle e_1 \pm e_2 - s \rangle C}\ [15]$$

$[e]$ I $\quad \dfrac{A \vdash_{K,U} B}{[e] \vdash_{K,U} [e-s] B} \qquad \dfrac{A, B' \vdash C \quad B, A' \vdash C \quad Bi, B'i \vdash C}{[e]B \wedge \bigwedge_1 [e1_i] Bi, [e]B' \wedge \bigwedge_1 [e2_i] B'_i \wedge \vdash [e] C}$

$\|$ I $\dfrac{p \vdash A \quad q \vdash B \quad A, B \vdash_{K,U} C}{p \| q \vdash_{K,U} C} \qquad$ Cut $\dfrac{A, B \vdash_{K,U} C \quad C \vdash_{K',U} D}{A, B \vdash_{K+K',U} D}$

[10] If $s \in \varphi(K)$ and $(e-s) \cap U = \emptyset$.
[11] If $s \in \varphi(K)$.
[12] Remark: $K \lceil V$ represents connections where actions of V do not participate.
[13] Same as footnote 10.
[14] Same as footnote 10.
[15] If $s \in \varphi(K)$ and $(e_1 + e_2) \cap U = \emptyset$.

Example 4.6. $\{a, b\}.\mathrm{nil} \parallel \{c\}\,\mathrm{nil} \vdash_{\{\langle a,c\rangle\},\{a,c\}} \langle b\rangle \mathrm{Tr}$

$$\dfrac{\dfrac{\dfrac{}{\mathrm{nil} \vdash_{\{\langle a,c\rangle\},\{a,c\}} \mathrm{Tr}}\,\mathrm{Ax}_1}{\{a, b\}.\,\mathrm{nil} \vdash_{\{\langle a,c\rangle\},\{a,c\}} \langle b\rangle \mathrm{Tr}}\,\langle e\rangle_5 \mathrm{I} \quad \dfrac{\dfrac{\dfrac{}{\mathrm{nil} \vdash_{\{\langle a,c\rangle\},\{a,c\}} \mathrm{Tr}}\,\mathrm{Ax}_1}{\{c\}.\,\mathrm{nil} \vdash_{\{\langle a,c\rangle\},\{a,c\}} \mathrm{Tr}}\,\langle e\rangle_5 \mathrm{I} \quad \dfrac{}{\mathrm{Tr}, \mathrm{Tr} \vdash_{\{\langle a,c\rangle\},\{a,c\}} \mathrm{Tr}}\,\mathrm{Ax}_3}{\{a, b\}.\,\mathrm{nil} \parallel \{c\}\,\mathrm{nil} \vdash_{\{\langle a,c\rangle\},\{a,c\}} \langle b\rangle \mathrm{Tr}}\,\parallel \mathrm{I}$$

4.2.2. Correctness and completeness of Sys_2

Theorem 4.7 (Correctness of Sys_2). *The proof system* Sys_2 *is correct i.e.,*

(i) *if* $p \vdash_{K,U} B$ *then* $p \models_{K,U} B$,

(ii) *if* $A, B \vdash_{K,U} C$ *then* $A, B \models_{K,U} C$.

Proof. Omitted.

Theorem 4.8 (Completeness of Sys_2). *The proof system* Sys_2 *is complete, i.e.*

if $p \models_{K,U} B$ *then* $p \vdash_{K,U} C$.

Proof. See Section 5.

5. Proofs of completeness of Sys_1 and Sys_2

5.1. Proof of completeness of Sys_1

The proof of completeness needs the following lemmas and proposition which are proved in [6].

Lemma 5.1. *If* $p \parallel q \models A$ *then there exist* C *such that* $p \models C$ *and* $C, q \models A$.

Proposition 5.2. *For a given* A *the set* $\mathscr{C}(A) = \{\mathscr{C}(p, q, A)\, p \models C$ *and* $C, q \models A\}$ *is finite.*

Lemma 5.3. *If* $A, p \parallel q \models B$ *and* B *not of the form* $[\underline{e}]C$ *then there exist* D *such that* $A, p \models D$ *and* $D, q \models B$.

Lemma 5.4. *If* $A, p \parallel q \models [\underline{e}]B$ *then there exist* $D1, D2$ *such that*

$$C1, q \models D1 \quad D1, q \models [\underline{e}]B.$$

$$C2, p \models D2 \quad D2, q \models [\underline{e}]B.$$

Lemma 5.5. (i) *If* $\mathrm{rec}\,x.p \models A$ *then there exist* n *such that* $(\mathrm{rec}\,x.p)^n \models A$.
(ii) *If* $A, \mathrm{rec}\,x.p \models B$ *then there exist* n *such that* $A, (\mathrm{rec}\,x.p)^n \models B$.

The proof of Theorem 4.8 is very technical. In fact it can be derived from the previous lemmas. For the readability of this paper we just illustrate a few cases. For the interested reader, the totality of the proof can be found in [6].

Case $(B = B1 \vee B2)$: If $A, p \models B1 \vee B2$ then $\forall r \models A\ r \| p \models B1$ or $r \| p \models B2$. We note $R1 = \{r \models A : r \| p \models B1\}$ and $R2 = \{r \models A\, r \| p \models B2\}$.

Let $A1 = A \wedge \bigvee_{r \in R1} \mathscr{C}(r, p, B1)$ and $A2 = A \wedge \bigvee_{r \in R2} \mathscr{C}(r, p, B2)$. We have $A1, p \models B1$ and $A2, p \models B2$. If $A1, p \models B1$ then by induction hypothesis there exist $D1$ such that $|A1| = |D1|$ and $D1, p \vdash B1$ and by $\vee$ I, $D1, p \vdash B1 \vee B2$. If $A2, p \models B2$ then by induction hypothesis $\exists D2$ such that $|A2| = |D2|$ and $D2, p \vdash B2$ and by $\vee$ I we have $D2, p \vdash B1 \vee B2$. By $\vee$ I, we have $D1 \vee D2, p \vdash B1 \vee B2$.

It remains to show that $|A1 \vee A2| = |A|$. Obviously $|A1 \vee A2| \subseteq |A|$. Conversely if $r \in |A1|$ then $r \| p \models B$ by instance $r \| p \models B1$ thus $r \models \mathscr{C}(r, p, B1)$ and then $r \in |A1|$, etc.

Case (B *of the form* $\langle e \rangle B$) *and* $p = e_1.q$: Two subcases are possible: either $e_1 = e$ or $e_1 \neq e$.

Subcase 1 $(e_1 = e)$: $A, e.q \models \langle e \rangle B_1 \Rightarrow \forall r \models A\ \ r \| e.q \models \langle e \rangle B1$. By operational semantics of the parallel operator: $\forall r \models A\ \ r \| q \models B1$ or $\exists r \xrightarrow{e} r'\ r' \| e.q \models B1$ or $\exists r \xrightarrow{\tau} r'\ r' \| q \models B1$.

We note $R1 = \{r \models A:\ r \| q \models B1\}$, $R2 = \{r \models A:\ \exists r \xrightarrow{e} r':\ r' \| e.q \models B1\}$ and $R3 = \{r \models A:\ \exists r \xrightarrow{\tau} r':\ r' \| q \models B1\}$ and let be $C1 = A \wedge \langle e \rangle \bigvee_{r \in R1} \mathscr{C}(r, q, B1)$, $C2 = A \wedge \bigvee_{r \in R2} \mathscr{C}(r, e.q, B1)$ and $C3 = A \wedge \langle e \rangle \bigvee_{r \in R3} \mathscr{C}(r', q, B1)$. $\bigvee_{r \in R1} \mathscr{C}(r, q, B1)$, $q \models B1$ then by induction hypothesis there exist $D1\,t$ such that $|D1| = |\bigvee_{r \in R1} \mathscr{C}(r, q, B1)|$ and $D1, q \vdash B1$. Then by $\langle e \rangle$ I,

$$D1\ e.q \vdash \langle e \rangle B1. \tag{1}$$

$\bigvee_{r \in R2} \mathscr{C}(r, e.q, B1)$, $e.q \models B1$ then by induction hypothesis there exists $D2$ such that $|D2| = |\bigvee_{r \in R2} \mathscr{C}(r, e.q, B1)|$. By $\langle e \rangle$ I, $\langle e \rangle D2$, $e.q \vdash \langle e \rangle B1$ and by $\wedge$ I, we have

$$A \wedge \langle e \rangle D2, e.q \vdash \langle e \rangle B1. \tag{2}$$

$\bigvee_{r \in R3} \mathscr{C}(r', q, B1)$, $q \models B$ then by induction hypothesis there exist $D3$ such that $\bigvee_{r \in R3} \mathscr{C}(r', q, B)| = |D3|$. By $\langle e \rangle$ I we have $\langle \tau \rangle D3$, $e.q \vdash \langle e \rangle B1$ and by $\wedge$ I,

$$A \wedge \langle \tau \rangle D3, e.q \vdash \langle e \rangle B. \tag{3}$$

From (1)–(3) and by $\vee$ I, we have $D1 \vee (A \wedge \langle e \rangle D2) \vee (A \wedge \langle \tau \rangle D3)$, $e.q \vdash \langle e \rangle B1$. $|A| = |C1 \vee C2 \vee C3| = |D1 \vee (A \wedge \langle e \rangle D2) \vee (A \wedge \langle \tau \rangle D3)|$ then $C = D1 \vee (A \wedge \langle e \rangle D2) \vee (A \wedge \langle \tau \rangle D3)$ is appropriate.

Subcase ($e_1 \neq e$): If $A, e_1.q \models \langle e \rangle B1$ then $\forall r \models A\ r \| e_1.q \models \langle e \rangle B1$. By operational semantics of parallel operator, we have: $\forall r \models A$: $\exists r \xrightarrow{e_2} r'$ such that $e = e_1 \pm e_2$ and $r' \| e_1.q \models B1$ or $\exists r \xrightarrow{e} r'$: $r' \| e_1.q \models B1$.
We note $R1 = \{r \models A: \exists r \xrightarrow{e} r': r' \| e_1.q \models B1\}$ and $R2 = \{r \models A: \exists r \xrightarrow{e_2} r': e = e_1 \pm e_2$ and $r' \| q \models B1\}$ and let $C1 = A \wedge \langle e \rangle \bigvee_{r \in R1} \mathscr{C}(r', e.q, B1)$ and

$$C2 = A \wedge \bigwedge_{e1 \pm e2 = e} \langle e_2 \rangle \bigvee_{r \in R2} \mathscr{C}(r', e_2.q, B1).$$

We have $\bigvee_{r \in R1} \mathscr{C}(r', e.q, B1)$, $e_1.q \models B1$. By induction hypothesis, there exist $D1$ such that $D1, e_1.q \vdash B1$ with $|\bigvee_{r \in R1} \mathscr{C}(r', e.q, B1)| = |D1|$. By $\langle e \rangle$I $\langle \underline{e} \rangle D1$, $e_1.q \vdash \langle e \rangle B1$ and by $\wedge$ I,

$$A \wedge \langle e \rangle D1, e_1.q \vdash \langle e \rangle B1. \tag{4}$$

$\bigvee_{r \in R2} \mathscr{C}(r', e_2.q, B1), q \models B1$. By induction hypothesis, there exist $D2$ such that $|D2| = |\bigvee_{r \in R2} \mathscr{C}(r', e_2.q, B1)|$ and $D2, q \vdash B1$. By $\langle e \rangle$I, $\langle e_2 \rangle D1, e_1.q \vdash \langle e \rangle B1$ and by $\wedge$ I, $\bigwedge_{e1 \pm e2 = e} \langle e_2 \rangle \bigvee_{r \in R2} \mathscr{C}(r', e_2.q, B1), e_1.q \vdash \langle e \rangle B1$ and by $\wedge$ I again

$$A \wedge \langle e_2 \rangle D1, e_1.q \vdash \langle e \rangle B1 \tag{5}$$

From (4) and (5) and by $\vee$ I, $(A \wedge \langle e \rangle D1) \vee (A \wedge \langle e_1 \rangle D2), q \vdash \langle e \rangle B1$.$C = (A \wedge \langle e \rangle D1) \vee (A \wedge \langle e_1 \rangle D2)$ is appropriate. □

5.2. *Proof of completeness of* Sys_2

The proof needs the following proposition, corollaries and lemmas which are proved in [6].

Lemma 5.6. *For all C, all K and all U there exist C′ such that for all p* $p[\![K]\!]\lceil U \models C$ *iff* $p \models C'$.

Corollary 5.7. *If* $A, B \models_{K+K',U} C$ *then there exist C′ such that* $p \models_{K,U} C'$ *and* $C' \models_{K',U} C$.

Corollary 5.8. *If* $p \| q \models_{K,U} A$ *then there exist B such that* $p \| q \models B$ *and* $B \models_{K,U} A$.

Lemma 5.9. *If* $\mathrm{rec}\, x.p \models_{K,U} A$ *then there exist n such that* $(\mathrm{rec}\, x.p)^n \models_{K,U} A$.

Lemma 5.10 (completeness of $A \models_{K,U} C$). *If* $A \models_{K,U} C$ *then there exist B such that* $|B| = |A|$ *and* $B \vdash_{K,U} C$.

Let L_{HML} be the set of HML formulas. NF is a subset of L_{HML} of normal forms and is inductively defined.

$D ::= C \mid C \vee D$
$C ::= E \mid G \mid E \wedge G \mid \mathrm{Tr} \mid \mathrm{Fal}$
$E ::= \langle b1\rangle D \wedge \langle b2\rangle D2 \wedge \cdots \wedge \langle bn\rangle D$
$G ::= [a1]D \wedge \cdots \wedge [an]D \quad ai \neq aj \text{ for } i \neq j$

Proposition 5.11. *If* $A \in L_{\mathrm{HML}}$, $\exists B \in \mathrm{NF}$ *such that* $m(B) \leqslant m(A)$ *and* $|A| = |B|$ *where* $m(B)$ *is the modal height of* B *and* $|B|$ *is the modal of* B.

Proof. Omitted. □

We now define a new proof relation $\Vdash_n$ on A, B, C where $A, B \in NF$ and $C \in L_{HML}$

$D, D' \Vdash_{K,U} A$ if $\forall C \in D, \forall C' \in D'$: $C, C' \Vdash_{K,U} A$
$C, C' \Vdash_{K,U} \mathrm{Tr}$
$C, C' \Vdash_{K,U} A$ if $C = \mathrm{Fal}$ or $C' = \mathrm{Fal}$
$C, C' \Vdash_{K,U} A \vee B$ if $C, C' \Vdash_{K,U} A$ or $C, C' \Vdash_{K,U} B$
$C, C' \Vdash_{K,U} A \wedge B$ if $C, C' \Vdash_{K,U} A$ and $C, C' \Vdash_{K,U} B$
$C, C' \Vdash_{K,U} \langle e\rangle B$ if $e \cap U = \emptyset$ and either $\langle e\rangle D \in C$ and $D, C' \Vdash_{K,U} B$, either $\langle e\rangle D' \in C'$ and $C, D' \Vdash_{K,U} B$, either $\langle e1\rangle D1 \in C$ and $\langle e2\rangle D2 \in C'$ and $D1, D2 \Vdash_{K,U} B$ such that $e = e1 \pm e2$.
$C, C' \Vdash_{K,U} [e]B$ if $e \cap U \neq \emptyset$ and $[a]E \in C$, $[b]E' \in C'$ either $[e]D \in C$ and $[e]D' \in C'$ and $D, C' \Vdash_{K,U} B$ and $C, D' \Vdash_{K,U} B$ either $[e1]D \in C$ and $[e2]D' \in C'$ such that $e1 \pm e2 = e \pm s$ and $s \in \varphi(K)$ and $D, D' \Vdash_{K,U} C$.

Lemma 5.12. $p \parallel q \models_{K,U} A \Rightarrow \exists D, D'$ *such that* $m(D \wedge D') \leqslant m(A)$ *and* $p \models D1$, $q \models D2$ *and* $D1, D2 \Vdash_{K,U} A$.

Lemma 5.13. $D, D' \Vdash_{K,U} A \Rightarrow D, D' \vdash_{K,U} A$.

Proof of Theorem 4.8. We prove that if $p \models_{K,U} A$ then $p \vdash_{K,U} A$. The proof is done by induction on A and p.

Case (A of the form Tr, Fal, $B \vee C$ and $B \wedge C$}: Straightforward.

Case (A of the form $\langle e\rangle B$): induction on p.

Subcase 1 ($p = \mathrm{nil}$): We never have $\mathrm{nil} \models_{K,U} \langle e\rangle B$

Subcase 2 ($p = e_1.q$): Then $e_1 = e \pm s$, where $s \in \varphi(K)$ and $q \models_{K,U} B$. By induction hypothesis $q \vdash_{K,U} B$ and by $\langle e\rangle \mathrm{I}$, $e.q \vdash_{K,U} \langle e\rangle B$.

Subcase 3 ($p = q + r$): Either $q \models_{K,U} \langle e\rangle B$ or $r \models_{K,U} \langle e\rangle B$. If $q \models_{K,U} \langle e\rangle B$ then by induction hypothesis $q \vdash_{K,U} \langle e\rangle B$ and $+\mathrm{I}$, $q + r \vdash_{K,U} \langle e\rangle B$. If $q \models_{K,U} \langle e\rangle B$ then by induction hypothesis $q \vdash_{K,U} \langle e\rangle B$ and by $+\mathrm{I}$, $q + r \vdash_{K,U} \langle e\rangle B$.

Subcase 4 ($p = \mathrm{rec}\, x.q$): By Lemma 5.9 there exist n such that $(\mathrm{rec}\, x.q)^n \models_{K,U} A$. By induction hypothesis $(\mathrm{rec}\, x.q)^n \vdash A$ and by rec I, $\mathrm{rec}\, x.q \vdash_{K,U} A$.

Subcase 5 ($p = q \| r$): By Lemma 5.12 there exist $D1$ and $D2$ such that $q \models D1$ $r \models D2$ and $D1$, $D2 \| = C$. By induction hypothesis $q \vdash D1$ $r \vdash D2$ and by Lemma 5.13, $D1, D2 \vdash A$ and finally by $\|$ I, $q \| r \vdash_{K,U} A$.

Subcase 6 ($p = q[\![K']\!]$): If $q[\![K']\!] \models_{K,U} A$ then $q \models_{K \cup K',U} A$. By induction hypothesis $q \vdash_{K \cup K',U} A$. By $[\![\ ]\!]$ I, $q[\![K']\!] \vdash_{K,U} A$.

Subcase 7 ($p = q\lceil V$): If $q\lceil V \models_{K,U} A$ then $q\lceil V[\![K]\!]\lceil U \models A$. Hence $q[\![K\lceil V]\!]\lceil U\lceil V \models A$ i.e. $q \models_{[K\lceil V],U \pm V} A$. By induction hypothesis $q \vdash_{K\lceil V,U \pm V} A$ and by $\lceil$ I, $q\lceil V \vdash_{K,U} A$.

Case (A *of the form* $[e]B$): Induction on p.

Subcase 1 ($p = \mathrm{nil}$): $\mathrm{nil} \vdash_{K,U} [e]B$ by Ax_2.

Subcase 2 ($p = e_1.q$). If $e \cap U \neq \emptyset$ then $e_1.q \vdash_{K,U} [e]B$ by Ax_4 else $e_1 = e \pm s$ for $s \in \varphi(K)$ and $q \models_{K,U} B$. By induction hypothesis, $q \vdash_{K,U} B$ and by $.I$, $e_1.q \vdash_{K,U} [e]B$.

Subcase 3 ($p = q + r$): $q \models_{K,U} [e]B$ and $r \models_{K,U} [e]B$. By induction hypothesis $q \vdash_{K,U} [e]B$ and $r \vdash_{K,U} [e]B$. By $+$I, $q + r \vdash_{K,U} [e]B$.

Subcase 4 ($p = \mathrm{rec}\, x.q$): Similar to subcase 4 of $A = \langle e \rangle B$.

Subcase 5: ($p = q \| r$): By Corollary 5.8 there exist C such that $q \| r \models C$ and $C \models_{K,U} A$. By Lemma 5.12, there exist $D1$, $D2$ such that $m(D1 \wedge D2) \leqslant m(A)$ and $q \models D1$ and $r \models D$ and $D1$, $D2 \models A$. By induction hypothesis, $q \vdash D1$ and $r \vdash D2$ and by Lemma 5.12, $D1, D2 \vdash C$. By Lemma 5.10, $C \vdash_{K,U} A$. By the cut rule, $D1, D2 \vdash_{K,U} A$ and finally by $\|$ I, $q \| r \vdash_{K,U} A$.

The *subcases* 6 and 7 for A of the form $[e]B$ are treated exactly as the *subcases* 6 and 7 for A of the form $\langle e \rangle B$. □

Conclusion, related work and future work

The problem of compositionality of modal assertions has been successfully dealt with by Stirling [18, 19, 20] and Winskel [21] who both give sound and complete compositional modal proof systems for CCS and SCCS. Here, we have shown, that the Stirling strategy can be successfully applied for the HAL process algebra. The proof system obtained for this algebra naturally looks like a CCS proof system and an SCCS system. It obviously differs from some axioms and rules. However, we have not treated the all-algebra HAL since value-passing is omitted. The modal proof system proposed in this paper remains valid when we consider value-passing without infinite branching. This is possible if we reduce the unification to the filtrage.

On the other hand, while the important question of compositionality is solved by this approach, it is still important to extend the results to more expressive logics. Work in this direction has already been done by Kim G. Larsen. In [10, 11], Larsen proposes a complete proof system for HML with recursion, in the spirit of those of C. Stirling and G. Winskel except that no structure on the processes is assumed.

In future work it would be interesting to combine compositionality with more expressive logics than HML.

References

[1] D. Austry and G. Boudol, Algèbre de processus et synchronisation, *Theoret. Comput. Sci.* **30** (1984) 91–131.

[2] H. Barringer, R. Kuiper and A. Pnueli, Now you may compose temporal logic specifications, in: *Proc. 16th ACM Symp. on Theory of Computing* (1984) 51–63.

[3] M. Belmesk, Z. Habbas and Ph. Jorrand, A process algebra over the herbrand universe, application to parallelism in automated deduction, in: U. Furbach, Ch. Suttner and B. Fronhöfer, eds., *Parallellizations in Inference*, LNAI Sub series of Lecture Notes in Computer Science (Springer, Berlin 1991) 163 181.

[4] J.A. Bergstra and J.W. Klop, Algebra of communicating processes, in: J.W. De Bakker et al., ed., *Proc. CWI Symp. Math and Comp. Sci.* (North-Holland, Amsterdam, 1986).

[5] E. Brinksma, Information processing systems, open systems interconnection, LOTOS. A formal description based upon the temporal ordering of observational behavior. Draft international standard ISO 8807, 1988.

[6] Z. Habbas, Une algèbre de processus pour un calcul basé sur la déduction. Thèse de doctorat, Alger, 1992.

[7] M. Hennessy and R. Milner, Algebraic laws for non deterministic and concurrency, *J. ACM* **32** (1) (1985) 137–161.

[8] C.A.R. Hoare, *Communicating Sequential Processes* (Prentice-Hall, Englewood Cliffs, NJ, 1985).

[9] Ph. Jorrand and Ph. Schnoebelen, Principles of FP2, term algebras for specification of parallel-machine, in: J.W. De Bakker, ed., *Languages for parallel architectures. Design, Semantics, Implementation, Models.* ch. 5 (Wiley, New York, 1989) 223–273.

[10] K.G. Larsen, *Compositional Theories Based on an Operational Semantics of Contexts*, Lecture Notes in Computer Science, Vol. 430 (Springer, Berlin, 1989) 87–518.

[11] K.G. Larsen, *Proof systems for satisfiability in Hennessy–Milner logic with recursion*, Theoretical Computer Science, Vol. 72 (North-Holland, Amsterdam, 1990) 265–288.

[12] K.G. Larsen, *Proof Systems for Hennessy–Milner Logic with Recursion*, Lecture Notes in Computer Science, Vol. 299 (Springer, Berlin, 1987).

[13] R. Milner, *A Calculus of Communicating Systems*, Lecture Notes in Computer Science, Vol. 92, 1980.

[14] R. Milner, Calculi for Synchrony and Asynchrony, *J. Theoret. Comput. Sci.* **25** (1983) 267–310.

[15] G. Plotkin, A structural approach to operational semantics, Lecture Notes, Aarhus University, 1981.

[16] Ph. Schnoebelen, Sémantique du parallélisme et Logique temporelle, Application au langage FP2, Thèse de doctorat INPG, juin, 1990.

[17] C. Stirling, *A complete Modal Proof System for a Subset of SCCS*, Lecture Notes in Computer Science, Vol. 185 (Springer, Berlin, 1985) 253–266.

[18] C. Stirling, *A Complete Modal Proof System for a Subset of CCS*, Lecture Notes in Computer Science, Vol. 194 (Springer, Berlin, 1985) 475–486.

[19] C. Stirling, Modal logics for communicating systems, *Theoret. Comput. Sci.* **49** (1987) 311–347.

[20] R. van Glabbeek, Comparative semantics and refinement of actions, Thesis, Centrum Voor Wiskunde en Informatica, Vrije Universiteit Amsterdam, 1990.

[21] G. Winskel, *A Complete Proof System for SCCS with Modal Assertions*, Lecture Notes in Computer Science, Vol. 206 (Springer, Berlin, 1985) 392–410.